

First Friday Fraud Facts

October 2, 2009

Share your stories

If you have a case you would like to see shared in *First Friday Fraud Facts*, please let us know.

QUESTIONS OR COMMENTS:

Erin Haney, CIA
Statewide Financial Internal
Controls Officer
155 Cottage St NE, U50
Salem, OR 97301

Phone: 503-378-3156 ext. 277

Fax: 503-378-3514

E-mail: erin.d.haney@state.or.us

Inside this issue:

Welcome	1
Assessing Fraud Risk	1
Fraud Risks and Controls	1
10-80-10 Rule	2
Fraud Case Overview	3
Training Opportunities	4

Welcome to First Friday Fraud Facts (F4). This edition will focus on some basic factors of fraud risk and control assessments and things you can do to increase fraud awareness.

ASSESSING FRAUD RISK

An effective fraud risk assessment program should be performed on a systematic basis. It is important to consider possible fraud schemes and scenarios, taking in to account both internal and external factors. The process should assess risk at all levels of the organization, entity-wide, as well as significant business units. Another important factor is to evaluate the likelihood and significance of each risk. Think about the key controls in place; who could take advantage of them and why.

Knowing your data is also a key factor in maintaining fraud awareness. It is important to know what the standard data within your organization looks like in order to identify possible red flags in the data.

FRAUD RISKS AND CONTROLS

Fraud risk exposure should be assessed regularly within an organization. This assessment will help identify potential schemes that could be perpetrated. Since these exposures may change overtime as the organization changes, it is important to update this assessment on a regular basis. There are several things to consider when assessing fraud risk and the controls that are in place to mitigate against fraud. Some suggestions are:

- Consider the risks and weigh the costs associated
- Know the controls in place and assess the weaknesses within those processes



- Identify who could potentially take advantage of the risks and weaknesses
- Be proactive in assessing what potential perpetrators of fraud could affect or do to carry out a fraud scheme
- Determine what some of the signs and signals (potential red flags) of fraud would be
- Identify and access sources of information to detect fraud
- Based on knowledge of the processes, assess what you would expect to see from the data that has been gathered
- Run tests and review results—compare these results to your expected outcome
- Evaluate, follow-up, and revise process as necessary.

This process should be an ongoing continuous process, and should change to adapt to changes within your organization as time goes on.

This list is not intended to be all inclusive; there are many other steps and processes that can be under taken to protect against and detect fraud. In addition, although these steps have the potential alert you to fraud, waste, or abuse within your organization, it is important to note that just because these processes are implemented does not guarantee every occurrence of fraud will be caught or stopped. These steps are merely a suggestion to mitigate against the chance of fraud, waste, or abuse occurring.

10-80-10 “RULE”

The 10-80-10 “rule” refers to a general assumption of the breakdown of the population and the likelihood of fraud occurrences.

- 10% of the population will NEVER commit fraud. This is the type of person that will go out of their way to return items to the correct party.
- 80% of the population might commit fraud given the right combination of opportunity, motivation, and rationalization. This is increasingly important given the current economic environment, and as new technologies emerge that allow for new opportunities to commit fraud.
- 10% of the population are actively looking at systems and trying to find a way to commit fraud.

A good fraud awareness campaign can help deter many potential instances of fraud. If you assume the 10-80-10 rule is accurate, then roughly 80% of the population could be deterred if they thought they would be caught. Therefore, creating a climate of fraud awareness and an active prevention and detection campaign could protect them from making a terrible mistake.

FRAUD CASE OVERVIEW

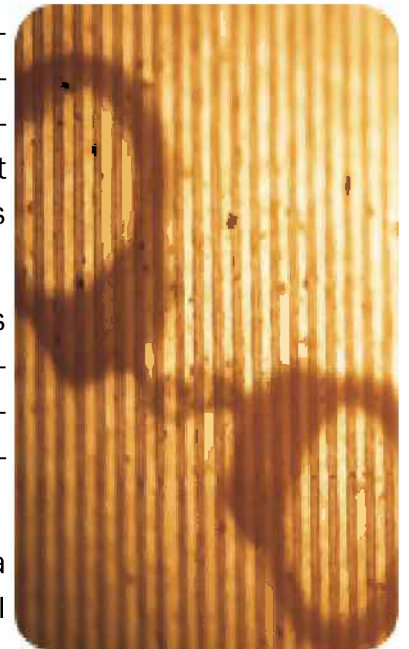
This case involves an identity theft scheme in which a mortgage company employee, and later government employee, was able to steal the identity of several individuals including several in conjunction with a disaster relief program.

Over a four year period, the perpetrator was able to steal the identity of over 200 individuals. The theft started when the perpetrator was an employee at a mortgage company and continued into later employment with a government entity. The individual was able to steal the victims information without the knowledge of the employer by copying their personal information from loan applications and applications for government assistance programs. Approximately 30 of the identity theft victims were applicants to government programs.

At least 74 of the stolen identities were used to open accounts with various retailers and fraudulently obtain credit in excess of \$156,000. The perpetrator used the credit to go on shopping sprees that included purchasing various items including jewelry, electronics, gourmet dinners, clothing, and various other items. The items were either kept for personal use or pawned at local pawn shops. Over the course of the four year period, dozens of items were pawned and the perpetrator was able to obtain over \$24,000 in cash.

The perpetrator blamed a drug problem as well as abuse as a child for his crimes. However, the judge in the case noted that drug addicts do not typically order gourmet food, such as steak and lobster, and that simple restitution would not undo the damage he had done to the victims credit and livelihoods.

The perpetrator faced a mandatory-minimum of two years in prison and a maximum of 32 years and a \$1,000,000 fine. Ultimately, the individual pleaded guilty to one count of wire fraud and one count of aggravated identity theft and was sentenced to 64 months in prison and ordered to pay over \$48,700 in restitution.



TRAINING OPPORTUNITIES



Internal Audit Quality Assessment: Performing an Internal or External Review

Date: November 2–4, 2009
Location: Oregon Department of Forestry—Santiam Room
2600 State St
Salem, OR 97310
Cost: \$300 IIA members/\$350 non-members
CPE: 19.5 credit hours

Participants will receive the most recent IIA Quality Assurance Manual, a \$200 value, FREE. For more information or to register visit: <http://www.theiia.org/chapters/index.cfm?cid=291>



Oregon State Fiscal Association training workshops

Two training workshops are available: session one is on Microsoft Access, session two is on ARRA Grants. Participants can attend one or both sessions.

Date: October 15, 2009
Time: 1:00–4:00 p.m.
Location: Salem Convention Center
200 Commercial St SE
Salem, OR 97301
Cost: \$30 for one session or \$50 for both
CPE: 1.5–3 credit hours

For more information or to register visit: <http://www.oregonstatefiscalassn.org/index.htm>

FIRST FRIDAY FRAUD FACTS IS PUBLISHED BY THE STATE CONTROLLER'S DIVISION

Statewide Financial Services
155 Cottage Street NE
Salem, OR 97301
Phone: 503-378-3156
Fax: 503-378-3514
<http://www.oregon.gov/DAS/SCD/>

WHO CAN YOU CALL FOR HELP?

The State Controller's Division reminds state agencies that it is always available to answer internal control questions. If you have an internal control problem or an audit finding and need help in resolving it, please contact:

Erin Haney
**Statewide Financial Internal Control
Officer**
erin.d.haney@state.or.us
503-378-3156 x277

Internal control tools are on the Web!

http://www.oregon.gov/DAS/SCD/internal_controls.shtml